Deploying the Barracuda Load Balancer with Office Communications Server 2007 R2

TECHNICAL NOTES

Organizations can use the Barracuda Load Balancer to enhance the scalability and availability of their Office Communications Server deployments.

Office Communications Server Overview

Organizations today use solutions like Microsoft Office Communications Server to allow them to effectively disseminate information and enhance collaborative efforts among their employees. Microsoft Office Communication Suite offers VoIP, instant messaging and Web collaboration among other capabilities. All these Services can be utilized by clients from either the internal office network or from the Internet.

Companies deploying Microsoft Office Communication servers for higher traffic throughput look to deploy a scalable solution. To scale the deployment of the Microsoft Office Communication Server solution Microsoft recommends using a hardware load balancer to distribute the traffic among multiple OCS servers.

Barracuda Networks has conducted interoperability tests between the Barracuda Load Balancer and Office Communications Server 2007 R2 (OCS). This document describes some ways to deploy the Barracuda Load Balancer to provide scaling in an OCS environment.

Prerequisites

- Microsoft Office Communications Server 2007 R2 Enterprise Edition
- Barracuda Load Balancer running firmware version 3.1.1.003 or higher
- *For Internal Office Communications Deployment:* Minimum one Barracuda Load Balancer, two recommended for high availability
- *For both Internal Office Communications Deployment and Edge Deployment:* Minimum two Barracuda Load Balancers, four recommended for high availability.

This document assumes that you have installed your Barracuda Load Balancer(s), have connected to the Web Interface, and activated your subscription(s). If you are planning to deploy Office Communications Server with high availability, you must first cluster your Barracuda Load Balancers. See the Barracuda Load Balancer Administrator's Guide for assistance with these steps.

Additional References

- Barracuda Load Balancer Administrator's Guide:
  - http://www.barracudanetworks.com/documentation/
- Technet Article on Load Balancing Enterprise Pools:
  - http://technet.microsoft.com/en-us/library/bb870398.aspx
  - http://technet.microsoft.com/en-us/library/dd572362(office.13).aspx
- Technet Article on Load Balancing Edge Servers with Enterprise Pools:
  - http://technet.microsoft.com/en-us/library/bb870418.aspx

Deployment Options

The supported deployments of the Office Communications Server and the Barracuda Load Balancer are described below.

Definitions	
Front-End Server	An OCS server in the internal network.
Edge Server	An OCS server deployed in the perimeter network.
Fully Qualified Domain Name (FQDN)	The unique name for a specific computer or host that can resolve to an IP address, e.g. www.example.com
Service	A combination of a virtual IP (VIP) address and one or more TCP/UDP ports that the Barracuda Load Balancer listens on. Traffic arriving over the specified port(s) is directed to one of the Real Servers associated with a particular Service.

OCS Front-End Server Deployment Options

Internal deployments are supported when deployed using a **one-armed** topology in either a single or multiple subnet configuration. Due to the design of communications between servers in an Office Communications Server enterprise pool, servers communicate with each other using the VIP address of the pool. To ensure the servers can communicate with each other, create a TCP Proxy Service and associate the servers with it.

Configurations that attempt to deploy internal OCS pools using a two-armed topology (Route-Path), Direct Server Return (DSR) or Bridge Mode are not supported and will cause many issues with communication between servers.

OCS Edge Server Deployment Options

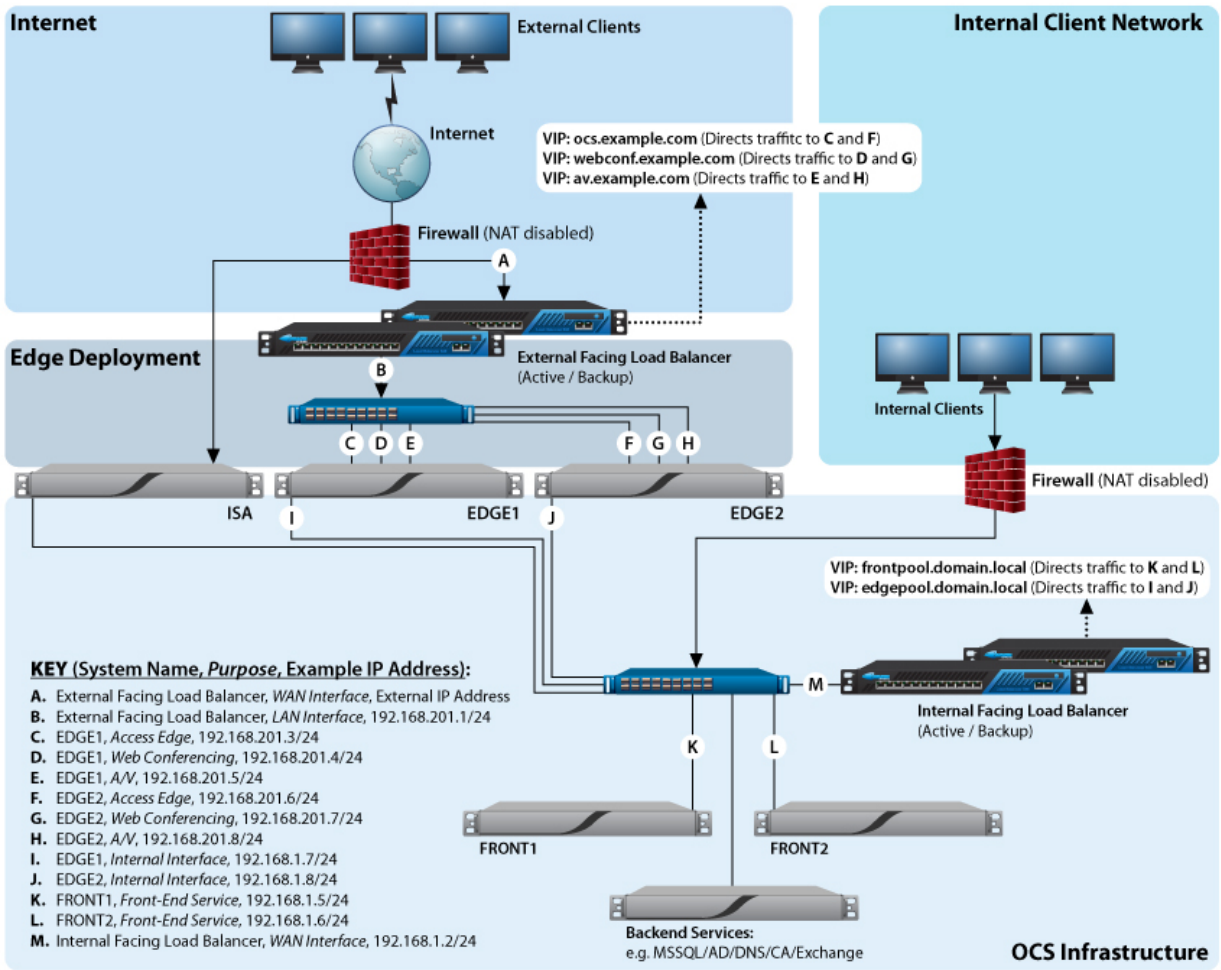
Load balanced Edge deployments are supported using either a **one-armed** topology using a TCP Proxy Service or a **two-armed** (Route-Path) topology using a Layer 4 Service. Bridge Mode and Direct Server Return deployments are untested and unsupported.

Deployment Example

Figure 1: OCS Deployment Example shows an example of a complete Office Communications Server deployment with Barracuda Load Balancers. This example is used in the deployment tasks that are detailed in the next sections.

Note that in this example, the Edge deployment uses a Route-Path topology while the Front-End deployment uses a one-armed topology.

Figure 1: OCS Deployment Example



Deployment Tasks

To deploy the Barracuda Load Balancer in an Office Communications Server environment, complete the following tasks. The rest of this document contains instructions for completing these tasks.

Task	Where
1. *Modify TCP and UDP Connections Settings.*	Do this on all active Barracuda Load Balancers, both internal and external. If your systems are clustered, the backup systems do not need to be configured separately
2. *Configure Front-End Services.*	Do this on the internal facing Barracuda Load Balancers.
If you have an *edge* deployment you must also do the following tasks:	
3. *Configure Internal Edge Services.*	Do this on the internal facing Barracuda Load Balancers.
4. *Configure External Edge Services.*	Do this on the Internet facing Barracuda Load Balancers.
5. *Confirm the Configure Edge Server Wizard.*	Check this on all Edge Servers.

Note: If your Barracuda Load Balancers are clustered, the configuration between the active and backup systems is synchronized. So, you do not need to modify any backup Barracuda Load Balancers.

1. Modify TCP and UDP Connections Settings

Do this on all active Barracuda Load Balancers, both internal (the Barracuda Load Balancer configured with the Front-End servers) and external (if there is a Barracuda Load Balancer deployed with Edge servers).

The Barracuda Load Balancer comes configured with settings that work with most applications. Office Communications Server has specific requirements that require changes to “expert” settings on the Barracuda Load Balancer to ensure it complies with Microsoft’s specifications. These settings are hidden by default.

To modify the TCP and UDP Connections settings on the Expert Variables page:

1. Click the **Advanced** tab in the Web Interface.
2. Append **&expert=1** to the end of the URL in the address bar of the browser, and press Enter to reload the page.
3. In the **Advanced Menu**, click the new tab in red named **Expert Variables.**
4. In the **TCP Connections Timeout** box, enter **1800** (30 minutes).
5. In the **UDP Connections Timeout** box, enter **1800** (30 minutes).

2. Configure Front-End Services

Do this on the internal facing Barracuda Load Balancers**.**

To configure all the Services needed for an internal OCS deployment, perform the following steps on the internal facing Barracuda Load Balancer:

1. Go to the **Basic > Services** page in the Web Interface.
2. For each port in the following table, add a Service. In the **Service Name** box, enter the name for the Service. In the **Virtual IP** box, enter the IP address for the FQDN of your Internal OCS Pool. In the **Port** box, enter the port for that Service in the table. In the **Real Servers** box, enter the IP address for every front-end server in your OCS Pool.

Service Name	Virtual IP Address	Protocol	Port	Real Servers
MTLS Front	IP for FQDN of Internal Enterprise OCS Pool e.g.192.168.1.11/24 for frontpool.domain.local	TCP	5061	IP Addresses of your Front-End Servers (K and L from the example)
DCOM WMI Front	IP for FQDN of Internal Enterprise OCS Pool e.g.192.168.1.11/24 for frontpool.domain.local	TCP	135	IP Addresses of your Front-End Servers (K and L from the example)
Internal Conf Front	IP for FQDN of Internal Enterprise OCS Pool e.g.192.168.1.11/24 for frontpool.domain.local	TCP	444	IP Addresses of your Front-End Servers (K and L from the example)
HTTPS Front	IP for FQDN of Internal Enterprise OCS Pool e.g.192.168.1.11/24 for frontpool.domain.local	TCP	443	IP Addresses of your Front-End Servers (K and L from the example)

3. For each Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. On the **Service Detail** page that appears:
   - In the **General** section, set the Service Type to **TCP Proxy**.
   - In the **Advanced Options** section, set **Session Timeout** to **0** (session never times out).

3. Configure Internal Edge Services

Do this on the internal facing Barracuda Load Balancers.

To configure all the Services needed for a load balanced OCS Edge Deployment, perform the following steps on the internal facing Barracuda Load Balancer:

1. Go to the **Basic > Services** page in the Web Interface.
2. For each port in the following table, add a Service. In the **Service Name** box, enter the name for the Service. In the **Virtual IP** box, enter the IP address for the FQDN of your Internal Edge OCS Pool. In the **Port** box, enter the port for that Service in the table. In the **Real Servers** box, enter the internal IP address for every Edge server.

Service Name	Virtual IP Address	Protocol	Port	Real Server
MTLS Edge	IP for FQDN of Internal Edge Enterprise OCS Pool e.g.192.168.1.12/24 for edgepool.domain.local	TCP	5061	Internal IP Addresses of your Edge Servers (I and J from the example)
AV Auth Edge	IP for FQDN of Internal Edge Enterprise OCS Pool e.g.192.168.1.12/24 for edgepool.domain.local	TCP	5062	Internal IP Addresses of your Edge Servers (I and J from the example)
RTP HTTP Edge	IP for FQDN of Internal Edge Enterprise OCS Pool e.g.192.168.1.12/24 for edgepool.domain.local	TCP	443	Internal IP Addresses of your Edge Servers (I and J from the example)
WebConf Edge	IP for FQDN of Internal Edge Enterprise OCS Pool e.g.192.168.1.12/24 for edgepool.domain.local	TCP	8057	Internal IP Addresses of your Edge Servers (I and J from the example)
RDP Media Edge	IP for FQDN of Internal Edge Enterprise OCS Pool e.g.192.168.1.12/24 for edgepool.domain.local	UDP	3478	Internal IP Addresses of your Edge Servers (I and J from the example)

3. For each **TCP** Service created, edit the Service by clicking the **Edit** graphic next to the Service entry in the table. In the **General** section, set the Service Type to **TCP Proxy**. In the **Advanced Options** section set **Session Timeout** to **0** (session never times out).
4. No change is required for the **UDP** Service (RDP Media Edge).

4. Configure External Edge Services

Do this on the Internet facing Barracuda Load Balancers.

To configure all the Services needed for a load balanced Edge Deployment of Office Communications Server, perform the following steps on the Internet facing Barracuda Load Balancer:

1. Go to the **Basic > Services** page in the Web Interface.
2. For each port in the following table, add a Service. In the **Service Name** box, enter the name for the Service. In the **Virtual IP** box, enter the IP address for the FQDN of your Internal Edge OCS Pool. In the **Port** box, enter the port for that Service in the table. In the **Real Servers** box, enter the internal IP address for every Edge server.

Service Name	Virtual IP Address	Protocol	Port	Real Server
Access Edge	IP for FQDN of Access Edge e.g. IP address for ocs.example.com	TCP	443	IP Address of Access Edge NICs on each Edge Server (C and F from the example)

WebConf Edge	IP for FQDN of WebConf Edge e.g. IP address for webconf.example.com	TCP	443	IP Address of WebConf NICs on each Edge Server (D and G from the example)
AV Edge	IP for FQDN of AV Edge e.g. IP address for av.example.com	TCP	443	IP Address of AV NICs on each Edge Server (E and H from the example)
AV UDP Edge	IP for FQDN of AV Edge e.g. IP address for av.example.com	UDP	3478	IP Address of AV NICs on each Edge Server (E and H from the example)

3. No further changes are required to these Services, as they all have type Layer 4 (the default).

5. Confirm the Configure Edge Server Wizard Setting

Check this on all Edge Servers.

When completing the **Configure Edge Server Wizard** you will see the **Internal Interface** dialog. The following note is displayed: "If you are using a load balancer, specify the IP address of the local server and the FQDN of the load balancer's VIP." In the **FQDN for the internal interface** box, enter the FQDN for the Access Edge DNS entry that external users will use.

If this is set correctly, then when the Edge Servers are queried for their host name strings, they will return the FQDN of the VIP address for the external Access Edge instead of the FQDN of the internal interface. This ensures that the SAN (Subject Alternative Name) on the certificate assigned to this internal interface for the Access Edge matches the Edge server's host string.

See *Figure 2: Configure Edge Server Wizard* for a screen shot of the wizard.

Figure 2: Configure Edge Server Wizard